

**UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

KIMBERLY THOMPSON, DUANE
HOPSON, JAMES LONG, and
SUZZETTE KATZMAN, on behalf of
themselves and all others similarly situated,

Plaintiff,

v.

KRISPY KREME DOUGHNUT
CORPORATION,

Defendant.

No.

COMPLAINT – Class Action

JURY TRIAL DEMANDED

Plaintiffs Kimberly Thompson, Duane Hopson, James Long, and Suzette Katzman, on behalf of themselves and on behalf of all others similarly situated, allege the following against Krispy Kreme Doughnut Corporation (“Defendant”) upon personal knowledge as to their own acts, and based upon their investigation, their counsel’s investigation, and information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the “Data Breach”), which held in its possession certain personally identifiable information (“PII”) and protected health information (“PHI”) (collectively, the “Private Information”) of Plaintiffs and other current and former employees of Defendant.

2. Defendant is a multinational doughnut and coffee house chain.

3. As a condition of their employment, Plaintiffs and Class Members provided their Private Information to Defendant.

4. Defendant owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Krispy Kreme utilized deficient data security practices, thereby allowing sensitive and private data to fall into the hands of strangers.

5. On November 29, 2024, Krispy Kreme became aware of unauthorized activity on its network systems.¹

6. On May 22, 2025, Krispy Kreme's investigation "determined that certain personal information was affected."² Krispy Kreme also claims that "[t]here is no evidence that the information has been misused, and [is] not aware of any reports of identity theft or fraud as a direct result of this incident."³

7. However, in December 2024, the Play ransomware group claimed responsibility for the data breach, allegedly stealing 164 gigabytes of data which it leaked on the Dark Web.⁴

¹ Krispy Kreme Notice of Data Breach, *available at* <https://www.krispykreme.com/notice-data-breach> (last accessed July 2, 2025).

² *Id.*

³ *Id.*

⁴ Eduard Kovacs, *161,000 People Impacted by Krispy Kreme Data Breach* <https://www.securityweek.com/161000-people-impacted-by-krispy-kreme-data-breach/> (last accessed July 2, 2025).

8. Defendant began notifying individuals of the breach on June 16, 2025.⁵

9. But for Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' PII and PHI, the Data Breach would not have occurred.

10. Defendant is well-aware that it is at high risk of attempted cyberattack due to the high value of the sensitive data.

11. Despite Defendant's awareness of both the value and sensitivity of the data it safeguarded and serious risk presented by insufficient security practices, Defendant did not take sufficient steps to ensure that its systems were secure. Defendant knew or should have known about the risk to the data it stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

12. The Data Breach was directly and proximately caused by Krispy Kreme's failure to implement reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII and PHI of over 160,000 individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiffs and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money,

⁵ Office of the Maine Attorney General, Data Breach Notifications, *available at* <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/0c411aee-5d5d-45bc-b6ad-ec41ce2bfdda.html> (last accessed July 2, 2025).

and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiffs and Class Members have lost the inherent value of their private data.

13. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit charges, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security. Likewise, the exfiltration of protected health information puts Plaintiffs and the Class Members at a present and continuing risk of medical identity theft, which poses an even more critical threat to victims because such fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

14. Moreover, Defendant's failure to notify Plaintiffs and Class Members that they had been impacted by this data breach for nearly seven months after Defendant became aware of the breach harmed Plaintiffs and made it more difficult for Plaintiffs to take swift action to respond to the breach.

15. Plaintiffs and Class Members have been harmed because they are at immediate risk of having their personal information used against them. Indeed, they have been at risk well before Defendant even notified Plaintiff of the breach. Plaintiffs do not

know if their data has been sold, transferred, replicated, or irrevocably disseminated and exposed. They suffered harm in the loss of the value of their data which cannot be easily recovered, if ever.

16. Plaintiffs, individually and on behalf of a nationwide class, allege claims of (1) Negligence, (2) Breach of Implied Contract; and (3) Unjust Enrichment. Plaintiffs also seek declaratory and injunctive relief. Plaintiffs ask the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiffs

17. Plaintiff Kimberly Thompson is and at all times mentioned herein a resident and citizen of Louisville, Kentucky.

18. Plaintiff Duane Hopson is and at all times mentioned herein a resident and citizen of Louisville, Kentucky.

19. Plaintiff James Long is and at all times mentioned herein a resident and citizen of Louisville, Kentucky.

20. Plaintiff Suzzette Katzman is and at all times mentioned herein a resident and citizen of East Bend, North Carolina.

21. Plaintiffs Thompson, Hopson, Long, and Katzman bring this case on behalf of themselves and all others similarly situated.

Defendant

22. Defendant Krispy Kreme is a Delaware-based corporation with its headquarters located in Winston-Salem, North Carolina.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Krispy Kreme. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendant through its business operations in this District, including the conduct giving rise to this Action. Defendant Krispy Kreme's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members from or within this District.

FACTUAL ALLEGATIONS

I. Background

26. Krispy Kreme is a multinational doughnut company and coffeehouse chain that operates in 40 countries and has 20,000 employees worldwide.⁶

27. As a condition of employment, Plaintiffs and Class Members were required to provide Private Information to Defendant.

28. Defendant's Privacy Policy states that "We take administrative, technical and organizational measures to protect your data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access."⁷

II. The Breach

29. Defendant learned of unauthorized access to its computer systems on November 29, 2024.

30. Through the Data Breach, the cybercriminal gained unauthorized access to highly sensitive Private Information, including "name, date of birth, Social Security number, driver's license or state ID number, financial account information, payment card information, passport number, digital signature, email address and password, biometric data, US military ID number, and medical and health information."⁸

31. On or around June 16, 2025, nearly seven months after Krispy Kreme learned of the Data Breach, Krispy Kreme began to notify Plaintiffs and other Class Members that

⁶ Catherine Muccigrosso, *Krispy Kreme sees lawsuits mount after data breach impacting over 160,000 people*, THE CHARLOTTE OBSERVER, <https://www.charlotteobserver.com/news/business/article309475265.html> (last accessed July 2, 2025).

⁷ Krispy Kreme Privacy Policy, *available at* <https://www.krispykreme.com/legal/privacy-policy> (last accessed July 2, 2025).

⁸ Krispy Kreme Notice of Data Breach, *available at* <https://www.krispykreme.com/notice-data-breach> (last accessed July 2, 2025).

their Private Information was viewed and taken by cybercriminals.

32. The Data Breach Notices do not provide details about the root cause of the Data Breach, the vulnerabilities exploited, the criminals responsible for the breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, Krispy Kreme has not explained or disclosed these facts to Plaintiffs and Class Members.

33. Without these details, Plaintiffs' and Class Members' ability to mitigate harms resulting from the Data Breach is severely diminished.

34. Defendant's Data Breach notice offers no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing credit monitoring, which is woefully inadequate considering the lifelong increased risk of fraud and identity theft that Plaintiffs and Class Members now face as a result of the Data Breach.

35. Defendant has offered only a limited one-year subscription for identity theft monitoring and identity theft protection through Kroll.⁹ Its limitation is inadequate when the victims will likely face many years of identity theft.

36. Moreover, Defendant's credit monitoring offer and advice to Plaintiffs and Class Members squarely place the burden on Plaintiffs and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiffs and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the Data Breach, Defendant

⁹ See *Exhibit*

merely sent instructions to Plaintiffs and Class Members about actions they could affirmatively take to protect themselves.

III. The Data Breach was Preventable

37. At all relevant times, Defendant knew, or should have known, that the PII and PHI it was entrusted with was a prime target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals for whom the exposure of the unencrypted data would harm.

38. As custodian of Plaintiffs' and Class Members' PII and PHI, Defendant knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred.

39. Defendant's security obligations were also especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI.

40. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹⁰ The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658),

¹⁰ 2021 Data Breach Annual Report, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed April 3, 2025).

compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

41. The United States' Cybersecurity and Infrastructure Agency ("CISA") and the FBI warned that since 2022, affiliates from the notorious cybercriminal group Play have "impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe."¹¹

42. The Play ransomware group "was among the most active ransomware groups in 2024."

43. The cybercriminals that obtained Plaintiffs' and Class Members' Sensitive Information appear to be from the Play ransomware group.¹²

44. In December 2024, the Play ransomware group claimed credit for the Data Breach on its Dark Web website.¹³

¹¹ #StopRansomware: Play Ransomware, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a> (last accessed July 3, 2025).

¹² Eduard Kovacs, *161,000 People Impacted by Krispy Kreme Data Breach* <https://www.securityweek.com/161000-people-impacted-by-krispy-kreme-data-breach/> (last accessed July 2, 2025).

¹³ *Id.*

45. Ransomware groups such as Play often post links to stolen data on a Data Leak Site (“DLS”).¹⁴ A DLS is a “website where the illicitly retrieved data of companies, that refuse to pay the ransom, are published.”¹⁵

46. However, even if a ransomware group removes stolen data from its DLS when a ransom is paid, there is no guarantee that the data will be deleted.¹⁶ The stolen Private Information is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.¹⁷

47. Ransomware groups can therefore monetize stolen Sensitive Information and sell it on the dark web as part of a full identity profile.¹⁸ Buyers can then use that information to conduct different types of identity theft or fraud, such as to file a fake tax return, to apply for a fraudulent mortgage or to open a bank account while impersonating the victim.¹⁹

¹⁴ Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, HIPAA JOURNAL (Feb. 23, 2024), <https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/#:~:text=While%20ransomware%20groups%20usually%20remove,little%20incentive%20to%20delete%20it>.

¹⁵ *Dedicated Leak Sites (DLS): Here’s what you should know*, GROUP-IB, <https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/> (last accessed April 3, 2025).

¹⁶ Adler, *supra* note 14.

¹⁷ *Id.*

¹⁸ Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, <https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion> (last accessed July 3, 2025).

¹⁹ *Id.*

48. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

49. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its customers' PII and PHI. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

IV. Defendant Failed to Comply with FTC Guidelines

50. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding its subscribers' PII and PHI, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII and PHI for a significant number of employees, a significant number of employees would be harmed by a breach of its systems. Defendant further knew that the data it was entrusted with was highly valuable and contained private and sensitive information including medical information.

51. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately

safeguarding PII held by businesses should be factored into all business-related decision making.

52. An FTC Publication titled “Protecting Personal Information: A Guide for Business” lays out fundamental data security principles and standard practices that businesses should implement to protect PII.²⁰ The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network’s vulnerabilities; and (e) implement policies to correct security problems.

53. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

54. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

55. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and

²⁰ See *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last accessed June 30, 2025).

appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

56. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

57. Defendant knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines.

58. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

59. Once Defendant became aware of the breach, it could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including taking *any* steps whatsoever to attempt to mitigate the harm caused by the breach.

60. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII

obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

61. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.²¹ Plaintiffs and Class Members generally have spent considerable time and stress in attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice’s Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims “reported spending an average of about 7 hours clearing up the issues.”²²

62. The information compromised in the Data Breach—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here,

²¹ *Identity Theft: Protect Yourself, Secure Your Future*, MARYLAND OFFICE OF THE ATTORNEY GENERAL, <https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf> (last accessed July 2, 2025).

²² Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEP’T OF JUSTICE, <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf>. (last accessed July 2, 2025).

however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual's medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Defendant subscribers at additional risk for potential medical fraud and medical identity theft.

63. Data breaches and disclosures involving medical records are not only incredibly costly, they can “also [be] more difficult to detect, taking almost twice as long as normal identity theft.”²³ The FTC warns that a thief may use private medical information to, among other things, “see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care”²⁴ and that this may have far reaching consequences for a victim's ability to access medical care and use insurance benefits.

V. Defendant Failed to Comply with Industry Standards

64. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

- a) Maintaining a secure firewall
- b) Monitoring for suspicious or unusual traffic on the website
- c) Looking for trends in user activity including for unknown or suspicious users
- d) Looking at server requests for PII

²³ See *What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed Nov. 22, 2023).

²⁴ *Id.*

- e) Looking for server requests from VPNs and Tor exit nodes
- f) Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII
- g) Structuring a system including design and control to limit user access as necessary, including a user's access to the account data and PII of other users.

65. Other best practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

66. Defendant failed to meet minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIC CSC), which are all established standards in reasonable cybersecurity readiness.

67. These frameworks are existing and applicable industry standards which Defendant failed to comply with.

VI. Plaintiffs' and Class Members' Experiences

Plaintiff Thompson

68. Plaintiff Kimberly Thompson is employed as an Assistant General Manager at Krispy Kreme's Louisville, Kentucky location.

69. Plaintiff Kimberly Thompson provided her sensitive PII and PHI to Defendant as a condition of employment with Defendant.

70. Plaintiff Thompson received notice of the Data Breach on or around June 16, 2025, informing her that her sensitive information was part of Defendant's Data Breach.²⁵

71. Plaintiff Thompson monitors her credit and bank accounts very closely and had a CreditKarma account before learning of the Data Breach.

72. A bank account was opened in the name of Plaintiff Thompson's husband at Chase Bank. Upon information and belief, neither Plaintiff Thompson nor her husband had opened this bank account.

73. Plaintiff Thompson has reported increased anxiety since learning of the Data Breach. She is frustrated that Krispy Kreme took seven months to inform her that her Private Information was leaked in the Data Breach even though she is a current employee, was aware of the Data Breach generally, and suffered the impacts of the Data Breach on her routine job duties.

74. The Data Breach hindered Plaintiff Thompson's job duties for at least two months. She said that after the Data Breach, many tasks were completed by hand, and employee payroll was often managed from employees' personal computers.

²⁵ See *Exhibit*

75. Plaintiff Thompson provided Defendant with her most sensitive medical and personal information and cannot be sure how much of it was exfiltrated.

76. Plaintiff Thompson suffered an actual injury in the form of damages and diminution in the value of her Private Information—a form of tangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

77. Plaintiff Thompson has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

78. Plaintiff Thompson has a continuing interest in ensuring that her Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Hopson

79. Plaintiff Hopson has worked as an employee of Defendant for five years.

80. Plaintiff Hopson provided his sensitive PII and PHI to Defendant as a condition of employment.

81. Plaintiff Hopson received notice of the Data Breach on or around June 16, 2025, informing him that his sensitive information was part of Defendant's Data Breach.

82. Prior to the Data Breach, Plaintiff Hopson has always taken reasonable precautions to protect his data, including credit monitoring and strong, unique passwords.

83. Plaintiff Hopson reported unauthorized charges on his CashApp credit card over the past few months. For example, he was charged for an Uber rideshare in the middle of a night on or around June 19, 2025. He did not request this Uber ride.

84. Plaintiff Hopson provided Defendant with his most sensitive medical and personal information and cannot be sure how much of it was exfiltrated.

85. As a result of the Data Breach, Plaintiff Hopson was forced to take measures to mitigate the harm, including changing his passwords and spending time monitoring credit and financial accounts.

86. Plaintiff Hopson has reported increased anxiety since learning of the Data Breach. He reports feeling lost and afraid to open additional accounts in case an unauthorized actor gains access to those new accounts. He also fears that he would not be able to reverse any future unauthorized charges or credit lines improperly opened in his name.

87. Plaintiff Hopson suffered an actual injury in the form of damages and diminution in the value of his Private Information—a form of tangible property that Plaintiff Hopson entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

88. Plaintiff Hopson has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

89. Plaintiff Hopson has a continuing interest in ensuring that his Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Long

90. Plaintiff Long received notice of the Data Breach on or around June 16, 2025, informing him that his sensitive information was part of Defendant's Data Breach.

91. Plaintiff James Long provided Defendant with his most sensitive medical and personal information and cannot be sure how much of it was exfiltrated.

92. Plaintiff Long suffered an actual injury in the form of damages and diminution in the value of his Private Information—a form of tangible property that Plaintiff Long entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

93. Plaintiff Long has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

94. Plaintiff Long has a continuing interest in ensuring that his Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Katzman

95. Plaintiff Katzman worked for Defendant in 2012 at its Winston-Salem, North Carolina store.

96. Plaintiff Katzman provided her sensitive PII and PHI to Defendant as a condition of employment with Defendant.

97. Plaintiff Katzman received a Data Breach Notice on or around June 16, 2025.²⁶

98. As per the Data Breach Notice's instructions, Plaintiff Katzman checked her credit.

99. A few days after receiving the Data Breach Notice, Plaintiff Katzman received an email impersonating Wood Forest Bank notifying her that another account had been opened in her name.

100. Plaintiff Katzman telephoned Wood Forest Bank's headquarters and learned that Wood Forest Bank did not send the letter. The bank representative advised her to mark the email as spam.

101. Plaintiff Katzman has reported increased anxiety since learning of the Data Breach because of the potential implications of her personal data being on the dark web. She feels as if something has been taken away from her. She also expressed surprise that her data remained in the system even though she worked for Defendant briefly over a decade ago.

102. Plaintiff Katzman suffered an actual injury in the form of damages and diminution in the value of her Private Information—a form of tangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data

²⁶ *See Exhibit*

Breach. Plaintiff Katzman suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

103. Plaintiff Katzman has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

104. Plaintiff Katzman has a continuing interest in ensuring that her Private Information, which upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

VII. Defendant Breached its Obligations to Plaintiffs and the Class

105. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information, out-of-pocket costs, and the time taken by Plaintiffs and Class Members to mitigate their injuries.

106. Plaintiffs and Class Members have been damaged by the compromise and exfiltration by cybercriminals of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of the Data Breach.

107. Plaintiffs and Class Members were damaged since their Private Information is being sold or potentially for sale by cybercriminals in the years to come.

108. As a direct and proximate consequence of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, actual, and substantial risk of harm

from fraud and identity theft, especially considering the actual fraudulent misuse of the Private Information that has already taken place.

109. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

110. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

111. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

112. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cybercriminals in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

113. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills

to insurance companies, or even undergo surgery under a false identity.²⁷ The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to “pay an average of \$13,500 to resolve the crime.”²⁸

114. As a direct and proximate result of Defendant’s conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

115. Many Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent charges;
- b. Cancelling and reissuing credit and debit cards;
- c. Purchasing credit monitoring and identity theft prevention;
- d. Monitoring their medical records for fraudulent charges and data;

²⁷ Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, available at <https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf> (last accessed Jan. 8, 2024).

²⁸ Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), <https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid>.

- e. Addressing their inability to withdraw funds linked to compromised accounts;
- f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- g. Placing “freezes” and “alerts” with credit reporting agencies;
- h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
- i. Contacting financial institutions and closing or modifying financial accounts;
- j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

116. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password protected.

117. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a Data Breach victim mitigate their injuries, and conversely, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach since November 2024, and did not notify all victims until June 2025.

CLASS ACTION ALLEGATIONS

118. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and those similarly situated.

119. Plaintiffs bring this class action on behalf of themselves and all other similarly situated individuals under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), on behalf of the following class (the "Nationwide Class") and, if appropriate, subclasses (the "State Subclasses"):

Nationwide Class

All individuals within the United States whose PII and PHI were exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 29, 2024.

Kentucky Subclass

All individuals within Kentucky whose PII and PHI were exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 29, 2024.

North Carolina Subclass

All individuals within North Carolina whose PII and PHI were exposed to unauthorized third parties as a result of the data breach discovered by Defendant on November 29, 2024.

120. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

121. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements therein.

122. **Numerosity.** The Nationwide Class is so numerous that the individual joinder of all members is impracticable. Defendant has reported to the Office of the Maine Attorney General that 161,676 individuals were affected by the Data Breach.

123. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

- a) Whether Defendant failed to take adequate and reasonable measures to ensure its website and data systems were protected;
- b) Whether Defendant failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;

- c) Whether Defendant unreasonably delayed in notifying subscribers of the harm they suffered once the suspicious activity was detected;
- d) Whether Defendant owed a legal duty to Plaintiffs and Class Members to protect their PII and PHI;
- e) Whether Defendant breached any duty to protect the personal information of Plaintiffs and Class Members by failing to exercise due care in protecting their PII and PHI;
- f) Whether Defendant's conduct violated Plaintiffs' and Class Members' privacy;
- g) Whether Defendant's conduct violated the statutes as set forth herein;
- h) Whether Defendant took sufficient steps to secure Class Members' Private Information;
- i) Whether Defendant was unjustly enriched;
- j) Whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,
- k) Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief or restitution.

124. **Typicality.** Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

125. **Adequacy of Representation.** Plaintiffs are adequate class representatives because they are Class Members, and their interests do not conflict with the Nationwide

Class's interests. Plaintiffs retained counsel who are competent and experienced in class action and data breach litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect their interests.

126. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

127. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests.

Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1

Negligence

On behalf of Plaintiffs and the Nationwide Class

128. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

129. Plaintiffs were required to provide PII and PHI as a precondition for receiving healthcare services from Defendant. Plaintiffs and Class Members entrusted their PII and PHI to Defendant with the understanding that it would safeguard their PII and PHI.

130. Defendant had full knowledge of the sensitivity of the PII and PHI that it stored and the types of harm that Plaintiffs and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

131. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify victims of the specific breached data in

a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

132. Defendant's duty of care arose from, among other things,

a) The special relationship between Defendant and its employees resulting from Plaintiffs and Class Members entrusting Defendant with confidential PII/PHI;

b) Defendant's exclusive ability (and Class Members' inability) to ensure that its systems, website, and vendor services were sufficient to protect against the foreseeable risk that a data breach could occur;

c) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

d) Defendant's common law duties to adopt reasonable data security measures to protect employee PII and PHI and to act under the same or similar circumstances as a reasonable and prudent person would act.

133. Plaintiffs and Class Members were the foreseeable victims of Defendant's inadequate data security. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches. Defendant knew that a breach of its systems or its contractors' systems could and would cause harm to Plaintiffs and Class Members.

134. Defendant's conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's conduct included its failure to adequately mitigate harm through

negligently failing to inform victims of the breach of the specific information breached for (as of time of writing) nearly seven months after the purported first discovery of the breach.

135. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI and the importance of limiting disclosure of that PII and PHI.

136. Defendant, through its actions and inactions, breached its duty owed to Plaintiffs and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in its possession and control. Defendant breached its duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices, failure to monitor the security of its networks and systems, and allowing unauthorized access to Plaintiffs' and Class Members' Private Information.

137. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

138. Defendant inadequately safeguarded consumers' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

139. But for Defendant's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen.

140. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach/unauthorized disclosure, and the harms suffered by Plaintiffs and Class Members.

141. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their Private Information had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

142. As a direct and traceable result of Defendant's negligence, Plaintiffs and Class Members suffered and will continue to suffer damages, including monetary damages, increased risk of future harm, loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach, overpayment for the services and products that were received without adequate data security; and embarrassment, humiliation, and emotional distress.

143. Plaintiffs and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiffs and Class Members are also entitled to the injunctive relief sought herein.

144. Plaintiffs also seek such other relief as the Court may deem just and proper.

Count 2

Negligence *Per Se*

On behalf of Plaintiffs and the Nationwide Class

145. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

146. Section 5 of the FTC Act, 15 U.S.C. § 45 prohibits, “unfair. . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiffs’ and Class Members’ Private Information.

147. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiffs’ and Class Members’ Private Information and by failing to comply with industry standards.

148. Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant’s systems. Plaintiffs were required to provide PII and PHI as a precondition for receiving employment from Defendant. Plaintiffs and Class Members entrusted their PII and PHI to Defendant with the understanding that it would safeguard their PII and PHI.

149. Class Members are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

150. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

151. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

152. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

153. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Count 3

Breach of Implied Contract

On behalf of Plaintiffs and the Nationwide Class

154. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

155. Plaintiffs and Class Members were required to entrust their Private Information to Defendant as part of the process of obtaining employment with Defendant.

156. Defendant solicited, offered, and invited Class Members to provide their Private Information in order to obtain employment with Defendant. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

157. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing employment to Plaintiffs and Class Members.

158. Plaintiffs and Class Members entrusted their Private Information to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect Private Information, and to timely and accurately notify Plaintiffs and the Class if their data has been breached and compromised or stolen.

159. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

160. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information, was Defendant's obligation to: (1) use such Private Information for business purposes only, (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' Private Information, (3) prevent unauthorized disclosures of the Private Information, and (4) retain Private information only under conditions that kept such information secure and confidential.

161. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiffs and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

162. Plaintiffs and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with the legal requirements, industry standards, and Defendant's own representations.

163. Implicit in the agreement between Defendant, Plaintiffs, and Class Members was the obligation that both parties would maintain information confidentially and securely.

164. These exchanges constituted an agreement and meeting of the minds between the parties.

165. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class Members would not have provided and entrusted their PII and PHI to Defendant in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiffs and Class Members was critical to realize the intent of the parties.

166. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

167. Defendant breached its implied contracts with Plaintiffs and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) failed to comply with industry standards; (3) failed to comply with the legal obligations necessarily incorporated into these agreements; and; (4) failed to notify Plaintiffs and Class Members of the specific data breached in a reasonably timely manner.

168. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

169. As a direct and proximate result of the breach/unauthorized disclosure, Plaintiffs and Class Members are entitled to relief as set forth herein.

170. Plaintiffs also seek such other relief as the Court may deem just and proper.

Count 4

Unjust Enrichment

On behalf of Plaintiffs and the Nationwide Class

171. Plaintiffs, individually and on behalf of the Class, incorporate by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

172. This count is brought in the alternative to Plaintiffs' breach of contract claim.

173. Plaintiffs and Class Members conferred a benefit on Defendant when they provided their Private Information to Defendant to obtain employment.

174. Upon information and belief, the monies paid to Defendant in the ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

175. Defendant, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

176. Defendant would not be able to carry out an essential function of its regular business without the money obtained in the ordinary course of business and Private Information provided by its employees. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

177. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

178. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

179. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have provided their Private Information to Defendant.

180. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and cheaper contractors and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

181. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiffs and Class Members conferred upon it.

182. Plaintiffs and Class Members have no adequate remedy at law.

183. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injuries that include one or more of the following:

ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

184. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members were underpaid by Defendant.

185. Plaintiffs also seek such other relief as the Court may deem just and proper.

Count 5

Injunctive/Declaratory Relief

On behalf of Plaintiffs and the Nationwide Class

186. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

187. Defendant owes a duty of care to Plaintiffs and Class Members, which required Krispy Kreme to adequately monitor and safeguard Plaintiffs' and Class Members' PII and PHI.

188. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiffs and Class Members.

189. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

190. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to adequately secure the PII and PHI of Plaintiffs and the Class within its care, custody, and control under the common law and Section 5 of FTC Act;

b. Defendant breached its duty to Plaintiffs and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiffs and the Class within Defendant's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiffs and the Class.

191. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the PII and PHI of Plaintiffs and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiffs and Class Members; and

b. Order that, to comply with Defendant's obligations and duties of care, Krispy Kreme must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII and PHI within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide services to its employees or customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

192. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs, Plaintiffs and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiffs and the Class for the serious risks of future harm.

193. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

194. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiffs and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

- A. That the Court certify this action as a class action and appoint Plaintiffs and their counsel to represent the Class;
- B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiffs and the Class by implementing improved security controls;
- C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

- D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;
- E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;
- F. That the Court award to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- G. That the Court award pre- and post-judgment interest at the maximum legal rate; and
- H. All such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial on all claims so triable.

Dated: July 3, 2025

Respectfully submitted,

/s/ Jean S. Martin

Jean S. Martin (N.C. Bar No. 25703)

Francesca K. Burne*

**MORGAN & MORGAN COMPLEX
LITIGATION GROUP**

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

Tel: (813) 559-4908

Fax: (813) 223-5402

jeanmartin@forthepeople.com

fburne@forthepeople.com

Amber L. Schubert*
**SCHUBERT JONCKHEER &
KOLBE LLP**
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: 415-788-4220
Fax: 415-788-0161
aschubert@sjk.law

*Counsel for Plaintiffs and
the Proposed Class*

*pro hac vice forthcoming